Despite uncertainty in the economy and jobs, our chapter remained strong throughout 2011. We started the year with 340 members and ended with 332. If 2012 improves in the areas that adversely affect membership, 2012 should show a significant growth and I believe it will.

One of our successes for 2011 was to have our ISSA Senior Members list swell to 16. Congratulations to those selected. The next round of Senior Member selections will be in May 2012, so if you have been a member of ISSA for 5 years please consider applying for selection.

The first meeting of the Board this year discussed publishing a calendar of events for planning purposes. A meeting schedule was accepted and will be placed on the chapter web site. This year we expect to finally change over our web site to a new format and updated software. It should make it easier to find information and keep it updated.

The first chapter meeting will be on Wednesday, January 18 at Bambino’s. It will be a luncheon from 11:00 – 1:00. VSS Monitoring, Inc. is sponsoring and providing a speaker. In February, the meeting will be at Bambino’s on February 22 from 5:30 – 7:30. Note that we will have evening meetings this year so more people can attend after work, so check the calendar and this newsletter to confirm the times.

As an outreach to security professionals who do not know of our chapter, members who cannot attend the luncheons and former members, the chapter has been sponsoring one hour (1 CPE) meetings at Schriever AFB on a monthly basis. Seven meetings have been held and word of mouth has spread the word. There are over 85 people at Schriever notified of the meetings and the list is growing. Cindy Thornburg (a new Senior Member) and Jeff Pettorino (Board member and ISSA Senior Member) are starting monthly meetings at Ft. Carson. We hope this will introduce more security professionals to the advantages of chapter membership and build a larger network of security professionals in the Colorado Springs area.

As 2012 unfolds this chapter will continue to grow, both in numbers and in the provided opportunities for the members. We will publish information in this newsletter, at meetings, and on our web site.

Thanks to our newsletter editor, Don Creamer, for putting together this communication opportunity for our chapter membership.

Mark Spencer
President
December 19, 2011: The U.S. government, apparently acting on more than the usual rumors or suspicions, is officially seeking information from companies in the telecommunications industry (service providers plus hardware and software manufacturers) about the use of Chinese made hardware and software. This investigation is trying to find out if Chinese espionage efforts include the use of communications hardware and software secretly modified to allow information to be secretly monitored and sent back to China. But many of the companies receiving the questionnaire are refusing to comply, because they fear that poor network security in U.S. government networks will allow others to steal questionnaire answers, and reveal company secrets. In response, the U.S. government invoked some Cold War era laws that compel answering the questionnaire on "national security" grounds.

This is but the latest effort to get a handle on the extent, if any, of Chinese spies using electronics and communications gear made in China to help steal American secrets. The fear began with the increased use of counterfeit Chinese electronic components. For several years now, it was believed that the illegal sale of Chinese made counterfeit computer components (microprocessors and related items) was part of an effort to gain secret access to U.S. government and military secrets.

Such counterfeit components ending up in American military equipment is old news. The fraud here is largely in the paperwork, where convincing looking counterfeit chips are labeled as "military grade" (the most robust and durable of that item available.) These sell for more than "consumer grade" (the most common) and "industrial grade" (for use in factories, where failure can cause more damage and expensive down time.) Failure in military grade parts can get people killed.

One reason China tolerates the widespread manufacture of counterfeit products is because some of them have some military benefit for China's Cyber War effort. Last year, for example, the FBI arrested two Americans for running a computer parts company that was selling counterfeit computer parts (especially Cisco router components), manufactured in China. The phony parts had counterfeit labels, and were delivered in counterfeit boxes. The two brothers had a contract to sell these parts to the Department of Defense and other government agencies. It was feared that the Chinese government could have some of these counterfeit chips equipped with a semi-magical "backdoor" that would enable an evil genius (or government bureaucrat) back in China to take control over equipment using the counterfeit part, and hooked up to the Internet. Or something like that. This is something the U.S. government is now trying to clarify, via the controversial questionnaires. So far, there have been no reports of backdoors discovered in Chinese hardware or software.

Actually, the Chinese got lucky with this one. Normally these counterfeit parts are sold by transitory operations. Eventually, the buyer has reason to contact the manufacturer of the shoddy part. At that point, the buyer discovers that, say, Cisco, has no router component with the serial number the scammed buyer is reading over the phone. It is then that the buyer realizes they have been screwed.

Of more immediate concern is not backdoors in counterfeit chips, but such secret features in legitimate chips or larger items (like routers and other hardware needed to operate the Internet). American engineers know that such secret features can be added to electronics. American espionage officials know that it can be done because the U.S. has already used this sort of thing, and has been doing so for decades. So it's not unreasonable to believe that the Chinese are catching up in this area as well. Exactly what is known about Chinese operations in this area is kept secret, because it is possible to send false information via this backdoor channel, but only if the Chinese believe their backdoors are still hidden from American view.

Meanwhile, counterfeit high-tech items are a growing business, and a grow-
Thank You 2011 Volunteers!!!

This Chapter could not function without you. Your help is greatly appreciated.

Jim Blake, Speaker, Providing future Web hosting
Donald Brackett, ISSEP Review Mediator
Ernest Calloway, Training Team Finance Manager
Arthur Cooper, Training Team Instructor
Don Creamer, Chapter Newsletter Production
Enrique de la Garza, Tabulated and reported Member Survey results
William (Wells) Fargo, Board Member, Generates and presents monthly challenge questions
Chuck Forth, AFCEA Liaison
Scott Frisch, ISC2 Exam Proctor, Contributed to ISSA/CTU Library
Mark Gerschefske, Training Team Instructor
Royal Harrell, Web Committee Chair, Training Team Instructor, Communications Officer
Rodney Hart, Training Team Instructor
Mark Heinrich, IEEE Liaison, Training Team Instructor
David Henson, Volunteer Coordinator
Joseph Hernandez, Training Team Instructor
Tim Hoffman, Executive Vice President, Career mentor
Deborah Johnson, Challenge Coin Committee Chair
Roy Kuwamoto, Tabulated and reported Member Survey results
Patrick Laverty, CTSC Liaison
Stephen Long, Contributes Hard monthly meeting questions
Wally Magda, Training Team Instructor

David Malone, Training Team Member
Craig McGuire, Web developer for future web site
Pamela Miller, Training Team Member, Refreshment coordinator
Albert Morse, Web committee member
Colleen Murphy, CISSP Coordinator, Training Team Instructor
Warren Pearce, Chapter Photographer
Jeff Pettorino, Social Media Coordinator, Board Member-at-Large
Sara Phillips, Web developer for future web site
Kevin Phillips, Web developer for future web site
OJ Pinckert, ISC2 Exam Proctor Alternate
Greg Playle, Training Team Instructor
George Proeller, Speaker, Advisor, Mentor
Barrett, Roshak, ISC2 Exam Proctor
Patrice Siravo, Training Team Instructor
Jim Stephens, Director of Training
Cindy Thornburg, Training Team Instructor
David Willson, Vice President, Colorado Springs Liaison, Training Team Instructor
Erik Wilmuth, ISC2 Exam Coordinator
Melody Wilson, Treasurer, Strategic Planning Committee Chair, Awards Committee Chair
Arthur Wilson, Awards Committee, Processed Chapter Surveys, Researched alternate meeting sites
Laura Woodworth, Chapter Recorder, Training Team Instructor
Validating Proprietary Digital Forensic Tools: A Case for Open Source

Digital forensic examiners rely on their expertise to interpret the data their tools retrieve. Although this requires utmost trust in the tools themselves, it also assumes that the tools are doing the job correctly. Not knowing how the tools do the job—not having access to their underlying code, as is the case with proprietary digital forensics tools—creates a veil of abstraction between examiners’ minds and the truth. Each layer of abstraction is a possible source for error or distortion.

That isn’t to say the conscientious examiner needs to cease use of any and all proprietary tools. However, it is important to validate what they find—to make sure results are repeatable (identical items tested by the same examiner, in the same lab, using the same equipment and methodology) and reproducible (identical items tested by different examiners, in different labs, using different equipment and methodology).

Performed at regular intervals, reproducible tests typically use one proprietary tool to validate another. For the purposes of the legal test known as the Daubert Standard, this is usually enough. However, the more attorneys on both civil and criminal sides learn about digital evidence, the more they may start questioning how forensic tools actually obtain their data. If the science underlying the evidence cannot be explained, then it cannot be accepted as a science, and the credibility of both digital evidence and digital forensic examiner will be undermined.

In some cases, the engineers who design proprietary forensic tools have been brought to court to testify as to how the tools work. However, this should only be a last resort; the designers of every proprietary tool an examiner uses may be unavailable, or prohibitively costly to bring to trial. There’s an easier, faster, and cheaper way to validate findings that use these tools. That way is to use open source forensic tools.

Read the rest of the article here:

Stolen, remote-wiped iPhones still get owner's iMessages. Victims of iPhone theft have discovered that remotely wiping their device will not stop iMessage content being delivered to the thief, who can continue to respond under the owner's name. The flaw was spotted by a man whose wife had her iPhone stolen and promptly deactivated the mobile number, remotely wiped the data, and changed both Apple ID and password. However, despite all the action taken, the husband discovered messages sent using iMessage were being received by the buyer of the stolen handset, in addition to being delivered to his wife's new handset, and shared the experience with Ars Technica. Not only was the receiver-of-stolen-goods getting messages addressed to the man’s wife, but the thief was able to respond to the messages. It appears the problem is not unique to the couple, but has hit many iPhone users, a problem which will presumably increase as iMessage gains ground. iMessage works by automatically turning SMS and MMS messages into Internet traffic when a data connection is available at both ends. It only operates where both parties have an iPhone, and are connected to the Internet, but when activated it does provide a free messaging service.

Source:
http://www.theregister.co.uk/2011/12/15/imessage_persistent/

Cashless Society: India Implements First Biometric ID Program for all of its 1.2 Billion Residents

Recently, India has launched a nationwide program involving the allocation of a Unique Identification Number (UID) to every single one of its 1.2 billion residents. Each of the numbers will be tied to the biometric data of the recipient using three different forms of information – fingerprints, iris scans, and pictures of the face. All ten digits of the hand will be recorded, and both eyes will be scanned.

The project will be directed by the Unique Identification Authority of India (UIDAI) under the premise of preventing identity theft and social welfare fraud. Fraud is a rampant problem in India, especially in relation to these programs due to a preponderance of corrupt politicians and bureaucrats who often stuff welfare rolls with fake names and take the money for themselves.

Social Media Security Considerations

Good information for the not-so-security-savvy in your organization:

- Use Common Sense!
- Don't divulge sensitive materials, photos or videos.
- Always think Operations Security. Every organization has something that doesn't need to be public knowledge.
- Be aware of the image you present when posting; remember, once posted, can't retract.
- Limit usage of social media to personal use only, do not write about work issues, always assume that everyone in the world is able to see what you write.
- Keep anti-virus software updated, run it regularly.
- Be cautious in how much personally identifiable information (PII) you disclose (employment organization and location, home address, home and business e-mail addresses, birth date, family member and pet names, phone numbers, social security numbers, photos, your schedule or routine (vacations, TDYs, day trips, shopping places visiting).
- Never assume you are in a trusted environment.
- Review your social media platforms' privacy settings, understand what information is collected and shared (pay attention to the site's privacy policies and terms) Default privacy settings are not private (set on high security).
- Avoid online games or quizzes that require you to provide personal information.
- Adhere to secure password guidelines (don't use same password for multiple social media sites and definitely not ones used at work).
- Exhibit caution in downloading third party applications.
- Log off when you are finished.
- Keep up with the latest social media scams.
- Google/Bing your name (and nickname) and check what information on you is online.
- Deactivate location-based (Geotags) including on your Smart phone.
- Do not log on to social media from public computers (Internet cafes).
- Always be skeptical and wary if someone asks to be your friend on social media.
- Do not automatically trust that posts are from who they claim to be.

Source—Defense Intelligence Agency

Backdoor Man

(Continued from page 2)

...ing danger. In addition to computer gear, auto and aircraft components are also being faked. Some aircraft and auto accidents have been traced to the fakes, which makes it a public safety issue. But with the Department of Defense installing counterfeit computer components, it becomes a national security issue. There's also the fear that the Chinese, or some other hostile nation, might get their hands on real computer components, and replace some of the chips with modified ones that will make government networks easier to hack. Yes, it just gets worse.

Chapter Officers:
Mark Spencer—Chapter President
Tim Hoffman—Executive Vice President
David Willson—Vice President
Melody Wilson—Treasurer
Royal Harrell—Communications Officer
Lora Woodworth—Recorder
Jeff Pettorino—Member at Large
William “Wells” Fargo—Member at Large

Position Chairs:
Deborah Johnson—Coins

The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Article for the Newsletter?
If you would like to submit an article...

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Can you interview one of the “movers and shakers”? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.

Send your article ideas to:
Don Creamer
(doncreamer@q.com)
Ensure that “Newsletter” is in the subject line. Looking forward to seeing you in print!

Upcoming Events

The January meeting will be on 18 Jan 2012 from 11:00 AM to 1:00 at Bambino's Bambino's Italian Eatery and Sports Bar, 2849 East Platte Avenue Colorado Springs, CO 80909-6238, (719) 630-8121.

The February meeting will be on 22 Feb 2012 from 5:30 to 7:30 also at Bambino's Bambino's Italian Eatery and Sports Bar.

SAVE THE DATE: Thursday, March 22, 2012— the March 2012 Conference, Crown Plaza Hotel, Colorado Springs,